State of Arizona

Department of Economic Security Information Technology Standards	Title: 1-38-0025 Access Control Policy	
Subject: This is the access control policy for access to DES confidential client, employee, employer information by authorized users	***Effective Date:*** **11/10/04**	***Revision:*** 1.1 04/27/05

1. **Summary of Standard Changes -** Original Implementation
   1.1. 04/27/05 - Added "This includes "00/00/00" logonid accounts where the user has not used the account for 90 days from the initial account setup."

2. Purpose

This policy is intended to provide an effective and efficient implementation of the DES Information Security Policy to ensure the protection of DES confidential data and the controlled access to that data.

3. Scope

This document encompasses all confidential DES data and all DES personnel and non-DES personnel who have access to DES data in performance of their duties; and all persons, DES and non-DES, who have the responsibility for maintaining and preserving DES data. Confidential data consists of, but is not limited to, data that can personally identify clients, employees, providers and employers.

4. Responsibilities

4.1. The DES Director, Deputy Directors, Associate Director, and Assistant Directors are responsible for enforcing this standard.

4.2. The DES CIO and the DES Division of Technology Services are responsible for implementing this DES standard.

5. Definitions and Abbreviations

5.1. Definitions

5.1.1. Confidential data consists of, but is not limited to, data that can personally identify clients, employees, providers and employers.

5.2. Abbreviations and Acronyms

5.2.1. CIO - Chief **I**nformation **O**fficer

5.2.2. DES – **D**ept of **E**conomic **S**ecurity

5.2.3. DSS – **D**atacenter **S**erver **S**upport

5.2.4. TS – **T**echnical **S**upport

5.2.5. ISA – **I**nformation **S**ecurity Administration

5.2.6. DSA – **D**ata **S**ecurity **A**nalyst

5.2.7. DSA – **D**ata **S**haring Agreement

5.2.8. UID – **U**ser **I**dentification **C**ode

5.2.9. LAN – **L**ocal **A**rea **N**etwork

5.2.10. WAN – **W**ide **A**rea **N**etwork

5.2.11. NSA – **N**ational **S**ecurity **A**gency

5.2.12. DTS - Division of **T**echnology **S**ervices

5.2.13. DES - Department of **E**conomic **S**ecurity

5.2.14. GITA - Government **I**nformation **T**echnology **A**gency

6. Policy

Confidential data maintained by DES must be protected by establishing and enforcing stringent access controls. Due to Federal and State security requirements, these controls must be managed by an authorized data security management system that is rated level C2 by the National Security Agency (NSA) in accordance with the Trusted Computer System Evaluation Criteria thus a *Trusted Product (see http://www.radium.ncsc.mil/tpep/epl/historical.html).*

6.1. General

6.1.1. Access Control Packages for Network-Connected Computers

All computers that can be reached by third-party networks (dial-up lines, extranets, the Internet, and so forth) must be protected by a privilege access control system approved by TS, DSS and ISA. This policy does not apply to computers that use modems to make outgoing dial-up calls, provided these systems do not receive unattended incoming dial-up calls.

6.1.2. Large Networks Must Be Divided into Separate Domains

All large networks crossing organizational boundaries must have separately-defined logical domains, each protected with suitable security perimeters and access control mechanisms.

6.1.3. Internet Commerce Servers Must Be in Demilitarized Zone (DMZ)

All Internet commerce servers, including payment servers, and web servers, must be protected by firewalls in a demilitarized zone.

6.1.4. Trusted Host Relationships Must Not Be Established Without Permission

Prior to enabling, TS, DSS and ISA must first approve in writing any trusted host relationships between computers connected to the DES internal network. A trusted host relationship involves the sharing of data files or applications across computers, or the elimination of the need to log on to more than one computer.

6.1.5. Trusted Host Relationships Prohibited for Internet Connected Machines

Unless approved by TS, DSS and ISA, all computers that are connected to the Internet or directly reachable through the Internet are prohibited from using shared directory systems, sometimes called shared file systems. These systems allow a user to obtain access to more than one computer's file system with only a single logon process. Exceptions are made for Internet commerce and other systems where a multi-machine architecture involves automatically passing users with severely restricted privileges from one computer to another.

6.1.6. Approval Required for Systems Accepting In-Coming Dial-Up Calls

Employees must not establish any communications systems, which accept in-coming dial-up calls unless these systems have first been approved by the TS and ISA.

6.2. Mainframe

All access to the mainframe shall be controlled by a logon process that includes a user logonid and password. Each logonid record will include a 10 position user identification code (UID). This UID code will contain information about the user creating a unique identification that allows access patterns as required by job responsibilities. The password will be an eight character alphanumeric expression that includes a minimum of one numeric character. All access shall be requested by the user's supervisor or manager and documented on a "Request for Computer Access" form J-125. In addition, all users must have a signed "User Affirmation Statement" J129 form on file with their respective data security office.

6.3. Network (LAN – WAN)

All access to a local or wide area network will be controlled by a logon process that includes a user logonid and password. The logonid will be unique to each individual user and conform to the requirements of the network operating system. The password will be an eight character alphanumeric expression that includes a minimum of one numeric character. (See section D2 below). All access shall be requested by the user's supervisor or manager and documented on a "Request for Computer Access" form J-125.

6.4. Operating System Access Control

6.4.1. Passwords Must Not Be Reused

Users must not be able to re-use a password for a history of six passwords. Administrators must not be able to re-use a password for a history of six passwords.

6.4.2. Passwords Must Contain Both Alphabetic and Non-Alphabetic Characters

All passwords must contain at least one alphabetic (at least one must be upper and one must be lowercase) and one non-alphabetic (numeric) character. Non-alphabetic characters include numbers (0-9). The use of control characters and other non-printing characters is prohibited because they may inadvertently cause network transmission problems or unintentionally invoke certain system utilities.

6.4.3. Periodic Forced Password Changes

All users must be automatically forced to change their passwords at least once every thirty (30) days. All administrator passwords must be changed every thirty (30) days.

6.4.3. Limit on Consecutive Unsuccessful Attempts to Enter a Password

To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password must be strictly limited. After three unsuccessful attempts to enter a password, the involved user-ID must be either: (a) suspended until reset by a security analyst, or (b) if dial-up or other external network connections are involved, disconnected.

6.5. Logonid Responsibilities & Procedures

6.5.1. Information Security Administration

The Information Security Administration shall create the logonid, the user identification code (UID) and the initial password for all non-DES users. The pre-requisite for access is an approved data sharing agreement between the outside non-DES entity and a DES Division(s) or Administration(s). As part of the process, the Data Security Administration shall forward the required access forms to the DES Divisions and/or Administrations included in the access. The Data Security Administration will be the repository for all original access forms and user affirmation statements submitted by non-DES entities.

6.5.2. Division and Administration Security Analysts

All Division and Administration Security Analysts shall create the logonid, the user identification code and the initial password for all members (employees, volunteers) of their Divisions or Administrations. The user identification codes shall be constructed to accurately reflect the identity of the user. The security analysts shall control access to their resources by creating and maintaining all resource rules and access rules within the security software. The security analysts shall provide access to non-DES users based on approved data sharing agreements and access forms sent by the Data Security Administration.

6.5.3. Network Administrators

All network administrators shall create the logonid, the initial password, and network access permissions for all members (employees, volunteers) of their Divisions or Administrations based on information provided to them by their data security staff.

6.6. Suspend & Unsuspend a Logonid

All logonids on the mainframe and networks shall be placed in suspend mode when they have not been used for 30 days. In addition, logonids shall be placed in suspend mode whenever it becomes known that an employee, volunteer, or authorized non-DES user will not be using the logonid for an extended period of time.

A logonid placed in suspend mode shall be unsuspended by the security staff, the network administrator and/or the help desk when contacted by the user and the user has been authenticated.

6.7. Removal of Logonid

All logonids and associated access shall be deleted within 1 business day when:

- the logonid has not been used for 90 days, , this includes “00/00/00” logonid accounts where the user has not used the account for 90 days from the initial account setup,
- the user has terminated or transferred and the supervisor has submitted deletion paperwork,
- the user is listed on the DES termination report.

Logonids may remain in suspend mode and not be deleted if there is documentation that the user is in a long term absence condition.

6.8. Password Reset

The password shall be reset by the security staff, the network administrator and/or the help desk when contacted by the user and the user has been authenticated.

6.9. Access Procedures

Access should be granted on the notion of least privilege. In other words, access should only be granted based only on what they need to know to do their jobs, and no more. This can be easily accomplished through the assignment of access based on roles.

7. Implications

7.1. Affected DES divisions and administrative entities may need to alter their operating procedures immediately to comply with this policy.

8. Implementation Strategy

8.1. All DES divisions and programs will implement this policy immediately.

9. References

9.1. None

10. Attachments

10.1. None

11. Associated GITA IT Standards or Policies

11.1. None

12. Review Date

12.1. This document will be reviewed twelve (12) months from the original adoption date, and every twelve months thereafter.